UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/576,516	05/23/2000	Xin Qiu	18926-002110US	4301

20350 7590 01/14/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/576,516	QIU ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/15/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26 and 28-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26 and 28-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-26, 28-32 remain are rejected under 35 U.S.C. 103(a) as being unpatentable over Grube et al. in view of Anderson, Jr.

3. As per claim 1, Grube et al. discloses a method of providing varying levels of security in a data processing system(405)(see fig. 4, sheet 3, col. 2, lines 39-57), receiving information from an outside source(see col. 2, lines 58-67, col. 3, lines 1-20); retrieving an indicator from the received information that instructs the system to operate at a higher level of security(see col. 3, lines 39-62, col. 5, lines 25-38). Grube et al. discloses to prevent operation at a lower level of security until information is received by the system to authorize a decrease in security levels, because if the acknowledgement is not received, or if the acknowledgement was not constructed with the proper transmission security level parameters, then the process ends(see col. 7, lines 53-65).

4. However, Grube et al. fails to disclose continuing operation of the processing system. Anderson, Jr. does disclose continuing operation of the processing system, because Anderson, Jr discloses that within a call made by an unauthorized user, the security level can be adjusted, either by increasing or decreasing the security level(see col. 12, lines 37-65).

5. It would have been obvious to one of ordinary skill in the art to combine Grube with Anderson, Jr. because both are analogous in the art of wireless communication. The motivation to combine Grube et al. with the feature of Anderson, Jr. that includes continuing operation of the processing system, is because it is highly desirable to have a new and improved security arrangement which requires the user to interact with the system to prevent access by an unauthorized user in such a manner that it would not be cost effective to defeat the security interposed for gaining access to the system(see col. 3, lines 36-43 of Anderson, Jr.).

6. As per claim 2, the same motivation applies above, also, Grube et al. discloses receiving an encrypted message(see col. 4, lines 7-20).

7. As per claim 3, Grube et al. discloses wherein said Decreased-Security Authorization-Code authorizes a decrease in encryption/decryption levels(see col. 3, lines 45-65).

8. As per claim 4, Grube et al. discloses wherein said Decreased-Security Authorization-Code authorizes a decrease in authentication level(see col. 3, lines 45-65).

9. As per claim 5, Grube et al. discloses wherein said Decreased-Security Authorization-Code authorizes a decrease in authentication level and a decrease in encryption/decryption levels(see col. 3, lines 45-65).

10. As per claim 6, Grube et al. discloses wherein said encrypted message further comprises a key for use in a decryption algorithm(see col. 4, lines 7-45).

11. As per claim 7, stores a master key(i.e. unique user key) to decrypt messages includes new decryption key values and using said master key stored at said system to decrypt said encrypted message(see col. 3, lines 59-67, col. 4, lines 1-45).

12. As per claim 8, Grube et al. discloses establishing a Security-Level-Status-Indicator at said system to indicate a level of security that is being implemented(see fig. 3, sheet 2).

13. As per claim 9, Grube et al. discloses said Security-Level-Status Indicator indicates a level of encryption/decryption that is being implemented by the system(see fig. 3, sheet 2, col. 3, lines 59-65, col. 5, lines 26-44).

14. As per claim 10, Grube et al. discloses said Security-Level-Status Indicator indicates a level of authentication that is being implemented by the system(see col. 3, lines 59-67).

15. As per claim 11, said Security-Level-Status Indicator indicates a level of authentication and a level of encryption/decryption that is being implemented by the system(see col. 3, lines 45-65).

16. As per claim 12, Grube et al. does not disclose configuring said Security Level Status Indicator to indicate more than two security levels so as to allow said system to utilize more than two security levels; however, the Examiner asserts that it would have been obvious to include Grube et al. to have more than two security levels, the motivation is that it increases security of the communication unit of Grube.

17. As per claim 13, Grube et al. does not disclose utilizing a cable head-end as said outside source; however, the Examiner asserts that it would have been obvious to utilize a cable head-end as an outside source, the motivation is that a cable head-end provides faster transmission.

18. As per claim 14, Grube et al. discloses using a Key Management Message to convey said Decreased Security Authorization Code(see col. 3, lines 45-65).

19. As per claim 15, Grube et al. discloses wherein delivery of said Key Management Message is authenticated(see col. 36-47).

20. As per claim 16, Grube et al. discloses wherein delivery of said Key Management Message is protected against a replay attack(see col. 7, lines 35-65).

21. As per claim 17, Grube et al. discloses wherein delivery of said Key Management Message is authenticated and protected against a replay attack(see col. 8, lines 1-30).

22. As per claim 18, Grube et al. discloses wherein a lower level of security is nonpublic Key mode, wherein a higher level of security is a public Key mode, continuing operation of the system in the public Key mode until an encrypted predefined message is received by the system from the outside source(see col. 3, lines 53-65).

23. As per claim 19, rejected under the same basis as claim 7.

24. As per claim 20, recites limitations already rejected(see claims 1 and 12).

25. As per claim 21, Grube et al. discloses a cryptographic device an input to receive a datastream; a Security -Level-Status-Indicator; and code means for executing a cryptographic algorithm wherein said cryptographic algorithm is indicated by said Security-Level-Status-Indicator(see col. 3, lines 59-67, col. 5, lines 26-44, fig. 3, sheet 2), and a code means for decrypting a decreased security authorization code(see col. 7, lines 24-35).

26. As per claim 22, Grube et al. discloses wherein said code means for executing a cryptographic algorithm comprises code means for executing a high level cryptographic algorithm and code means for executing a low level cryptographic algorithm relative to said high level cryptographic algorithm(see fig. 3, lines 59-67).

27. As per claim 23, Grube et al. discloses wherein said high level cryptographic algorithm comprises a high level decryption algorithm and wherein said low level cryptographic algorithm comprises a low level decryption algorithm(see col. 3, lines 53-65).

28. As per claim 24, Grube et al. discloses wherein said high level cryptographic algorithm comprises a high level authentication algorithm and wherein said low level cryptographic algorithm comprises a low level authentication algorithm(see col. 7, lines 24-35).

29. As per claim 25, Grube et al. discloses wherein said high level cryptographic algorithm comprises a high level decryption algorithm and a high level authentication algorithm and wherein said low level cryptographic; algorithm comprises a low level decryption algorithm and a low level authentication algorithm(see col. 3, lines 59-67, col. 7, lines 24-35) .

30. As per claim 26, Grube et al. discloses wherein said high level cryptographic algorithm is a public Key encryption algorithm and wherein said low level cryptographic algorithm is a non-public Key encryption algorithm(see col. 3, lines 53-65).

31. As per claim 28, Grube et al. discloses and means for preventing a replay attack in delivery of said Decreased-Security Authorization-Code(see col. 8, lines 1-30).

32. As per claim 29, Grube et al. discloses a master key to use in decrypting said Decreased Security Authorization Code(see col. 3, lines 59-67, col. 4, lines 1-45).

33. As per claim 30, Grube et al. discloses wherein said Security Level Status Indicator is encrypted(see col.7, lines 36-50).

34. As per claim 31, Grube et al. discloses providing a receiver to receive a transmission(see col. 2, lines 58-67, col. 3, lines 1-20); establishing a Security-Level-Status-Indicator at said receiver(see col. 3, lines 59-67); establishing a first level of decryption at said receiver(see col. 3, lines 59-67, col. 4, lines 1-20); encrypting a first message at a first level of encryption(see col. 3, lines 59-67, col. 4, lines 1-20); transmitting said first message to said receiver at said first level of encryption(see col. 2, lines 58-67, col. 3, lines 1-20); receiving said first message at said

receiver(see col. 7, lines 36-65); decrypting said first message encrypted at said first level of encryption(see col. 7, lines 36-65); transmitting a Decreased-Security-Authorization Code to change from said first level of decryption to a second level of decryption(see col. 3, lines 12-58); receiving said Decreased-Security-Authorization-Code; determining a change in encryption level from said first level of encryption to said second level of encryption(see fig. 3, lines 59-67, col. 4, lines 1-20); adjusting said Security-Level-Status-Indicator at said receiver(see fig. 3, sheet 2); encrypting a second message at said second level of encryption(see col. 3, lines 59-67, col. 4, lines 1-5); transmitting said second message at said second level of encryption; receiving said second message at said receiver; and decrypting said second message at said receiver(see col. 4, lines 7-20, 49-67).

35. As per claim 32, it is rejected under the same basis as claim 31.

Response To Amendment

36. Applicant's arguments filed 10/15/2004 have been fully considered but they are not persuasive.

37. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Anderson discloses continuing operation of the processing system, because

Anderson discloses that the within a call made the security level can be adjusted either by increasing or decreasing the security level(see col. 12, lines 37-65).

38. The Applicant states that Grube does not disclose a decreased security authentication code that is a code applicable to authorize a change in security from a higher level of security to a lower level of security. The Examiner disagrees with the Applicant. Grube discloses that the security gateway will also determine a unique user key based on the identity of the requester or requesting communication unit, but the security gateway can also have a dynamic key algorithm that is able to communicate the security level information to the communication unit(see col. 3, lines 59-67, col. 4, lines 1-6).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

January 8, 2005

AU2131
1/10/05